

PTH:RAS
F.#2020R00342

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF A
DARK BLUE MOTOROLA PHONE, PETS
NO. 1203550594, CURRENTLY LOCATED
AT THE NYPD PROPERTY CLERK'S
OFFICE IN RICHMOND COUNTY,
WITHIN THE EASTERN DISTRICT OF
NEW YORK

APPLICATION FOR A SEARCH
WARRANT FOR AN ELECTRONIC
DEVICE

Case No. 20-MJ-922

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, STEVEN KAPLAN, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the United States Attorney's Office for the Eastern District of New York, and have been since 2009. Prior, I was a law enforcement officer with the New York City Police Department (the "NYPD") from 1985 through 2009, including a period of time in the NYPD (i) robbery task force from 1986 through 1988; (ii) narcotics division from 1988 through 1993; and (iii) cold case squad from 1994 through 2009. I have been involved in the investigation of numerous cases involving the illegal trafficking distribution and possession

of narcotics. I have also received training on the uses and capabilities of cellular telephones in connection with criminal activity.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a dark blue Motorola phone, vouchered at PETS No. 1203550594, hereinafter the “Device.” The Device is currently located at the NYPD Property Clerk’s Office in Richmond County, within the Eastern District of New York.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On or about September 16, 2020, a grand jury in the Eastern District of New York returned an indictment charging defendant Ralph Livingston with distribution and possession with intent to distribute cocaine base and conspiracy to do the same in violation of Title 21, United States Code, Sections 841 and 846 (the “Subject Offenses”). (See 20-CR-370, ECF Docket No. 1.)

7. The charges are based on the defendant’s sales of narcotics to an undercover law enforcement officer (the “UC”) in March and April of 2020.

8. During the course of these transactions, five of which are charged in the Indictment, the UC communicated with the defendant by contacting the defendant on a phone

that, according to subpoenaed records, has been subscribed to Ralph Livingston since August 27, 2015. The UC communicated with the defendant on that phone both through telephone calls as well as through text messages to coordinate narcotics transactions, including discussing meeting times and locations, as well as drug quantities and prices.

9. For example, on or about March 2, 2020, the UC sent a text message to the defendant stating, “Can u do 5g[.] For tomorrow like 12,” to which the defendant responded, “Yeah, 65 a gram!” On or about March 10, 2020, the defendant sent a text message to the UC stating, “My people’s let me know that best they can do is \$60 a t-shirt! That would be \$1200 for 20 t-shirts[.]” Shortly after this text communication, the UC began purchasing 20 grams of crack cocaine from the defendant in a single transaction. On or about May 28, 2020, the defendant sent a text message to the UC that stated, “20=\$1200, 30=\$1800.” Based on my training and experience, I understand these messages to relate to the price and quantity of narcotics and I understand the term “t-shirt” to be a code for narcotics.

10. In addition, on March 17, 2020, the UC observed the defendant call an individual the UC understood to be the defendant’s narcotics supplier. Specifically, during a narcotics buy on March 17, 2020, the defendant entered the UC’s vehicle and, after directing the UC to a location, the defendant indicated to the UC that the defendant was going to call “him.” The UC understood “him” to refer to the defendant’s narcotics supplier. The defendant then made a phone call and informed the person on the phone that he was “coming for ten right now” and would “come right back for the other ten.” During this buy, the UC purchased 20 grams of crack cocaine (a substance containing cocaine base). The UC provided the defendant with part of the payment, and the defendant then left the car and returned with approximately ten grams of

narcotics. The UC then gave the defendant the remainder of the payment, after which the defendant left again and returned with the remainder of the narcotics.

11. Similarly, on March 24, 2020, during an attempted buy, the defendant again called an individual the UC understood to be his narcotics supplier in the UC's presence. After speaking on the phone, the defendant informed the UC that he needed more time to obtain the narcotics. The defendant later sent a text message to the UC and asked if they could meet the following day instead. An undercover buy took place the following day.

12. The UC most recently contacted the defendant on that same phone number in July of 2020.

13. On or about September 23, 2020, the defendant was arrested for unrelated narcotics possession and was arraigned in the state courts. At the time of his arrest, the defendant was in possession of the Device and was not in possession of any other phones.

14. Based on my training and experience, I know that narcotics traffickers often store on electronic devices photographs or videos of co-conspirators, narcotics, currency, stash houses and other locations or paraphernalia related to narcotics trafficking. I also know that narcotics traffickers often communicate with co-conspirators by phone, including through voice and messaging applications.

15. Based on my training and experience, I also know that narcotics traffickers often maintain records and contacts on electronic devices relating to their narcotics trafficking business. This includes, but is not limited to: (i) contacts and other information regarding customers and co-conspirators, including information that can assist in identifying those

individuals; (ii) information regarding the source or destination of trafficked narcotics; (iii) information relating to the narcotics trafficker's and his or her co-conspirators' schedules, travel or locations, that reflects the transport or storage of narcotics or currency related to the narcotics trafficking business; and (iv) records of the narcotics trafficking business, including records relating to the type, quantity and price of narcotics, as well as details relating to specific narcotics-related transactions.

16. Based on my training, experience and participation in other narcotics investigations, I know that individuals involved in narcotics trafficking often maintain on electronic devices financial records, just as others do who are not involved in illegal conduct. In the case of narcotics traffickers, this financial information often constitutes evidence of narcotics trafficking as it may reflect the location, transfer or amount of proceeds of the narcotics trafficking business.

17. Based on the foregoing the is probable cause to believe that the Device is the phone the defendant used to communicate with the UC and with his narcotics supplier. There is also probable cause to believe that there is evidence of the Subject Offenses on the Device.

18. The Device is currently in the lawful possession of the NYPD. It came into the NYPD's possession when it was seized incident to the defendant's September 23, 2020 arrest. Therefore, while the NYPD might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

19. The Device is currently in storage at the NYPD Property Clerk's Office in Richmond County, within the Eastern District of New York. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the NYPD.

TECHNICAL TERMS

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also

include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some

GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

21. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

26. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

27. It is respectfully requested that this Court issue a limited order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant, except that the materials may be produced as discovery as appropriate in United States v. Livingston, 20-CR-370 (FB), and may be provided to the Richmond County District Attorney's Office to be used in Richmond County Criminal Court Case No. CR-003299-20RI (the "State Case"), and to be produced as discovery as appropriate in the State Case. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into a criminal organization and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit

and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Steven Kaplan

Steven Kaplan
Special Agent
United States Attorney's Office

Subscribed and sworn to before me by telephone
on October 7, 2020

Vera M Scanlon

THE HONORABLE VERA M. SCANLON
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is a dark blue Motorola phone, vouchered at PETS No. 1203550594, hereinafter the “Device.” The Device is currently located at the NYPD Property Clerk’s Office in Richmond County, within the Eastern District of New York

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 21, United States Code, Sections 841 and 846 and involve Ralph Livingston since January 1, 2020, including:

- a. Communications with co-conspirators;
- b. lists of customers and related identifying information;
- c. types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;
- d. any information related to sources or destinations of drugs (including names, addresses, phone numbers, or any other identifying information);
- e. any information recording Ralph Livingston's and his co-conspirators' schedules, travel or locations;
- f. any images or videos of narcotics, narcotics paraphernalia, currency, stash houses and co-conspirators; and
- g. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.